CLAIMS

1. Method for communicating to a server machine (2b) a certificate of a user (4) sent by a client machine (2a) via a security module (2c) of a computer system (1), the protocol used between the machine (2a) and (2b) being HTTP or an equivalent protocol, a security protocol like SSL or an equivalent protocol being implemented between the client machine (2a) and the security module(2c), characterized in that it consists of inserting said certificate into a cookie header of a request in HTTP or an equivalent protocol in order to transmit them from the security module (2c) to the server machine (2b).

2. Method according to claim 1, characterized in that it consists of removing from said certificate all of the separators used in the headers of the HTTP messages prior to its insertion into a cookie header.

3. Method according to either of claims 1 and 2, characterized in that it consists of searching, prior to the insertion of said certificate into a header, to see if a cookie header is present in the HTTP request sent by the client machine (2a) and if not, of creating one.

4. Method according to claim 3, characterized in that it consists of adding a specific cookie into the existing or created cookie header, a configurable default name being assigned to said specific cookie enabling the server machine (2b) to distinguish the certificate from the cookies of the HTTP or equivalent request.

5. Method according to any of claims 1 through 4, characterized in that it consists of transmitting to the server machine (2b) the HTTP or equivalent request sent by the client machine (2a) into which the certificate has been inserted.

6. Security machine (2c) for securing the exchanges between a client machine (2a) and a server machine (2b) of a computer system (1), the protocol used between the machine (2a) and (2b) being HTTP or an equivalent protocol, a security protocol like SSL or an equivalent protocol being implemented between the client machine (2a) and said

security machine (2c), characterized in that it comprises analyzing means (6) that make it possible to transmit a certificate into a cookie header of an HTTP or equivalent request.

7. System comprising a client machine (2a), a server machine (2b) and a security module (2c), the protocol used between the machine (2a) and (2b) being HTTP or an equivalent protocol, a security protocol like SSL or an equivalent protocol being implemented between the client machine (2a) and the security module (2c), characterized in that the security module (2c) comprises analyzing means (6) that make it possible to transmit a certificate sent by the client machine (2a) into a cookie header of an HTTP or equivalent request.

8. Program integrated into a security module (2c) that allows the method according to any of claims 1 through 5 to be executed when the program is run in a machine.